JOURNAL OF NUMBER THEORY 12, 447–459 (1980)

Sur la factorisation des polynômes $f(X^{p^{2r}} - aX^{p^r} - bX)$ sur un corps fini $\mathbb{F}_{p^s}$

SIMON AGOU

Département de Mathématiques, Université Claude-Bernard Lyon 1, 43, Boulevard du 11 Novembre 1918, 69621, Villeurbanne, France

Communicated by P. Roquette

Received July 6, 1979

On détermine explicitement pour $p \neq 2$, le plus petit des degrés des irréductibles de $\mathbb{F}_{p^s}[X]$ factorisant le polynôme $f(X^{p^{2r}} - aX^{p^r} - bX)$.

INTRODUCTION

Soient $f(X)$ un polynôme irréductible de $\mathbb{F}_{p^s}[X]$ de degré n et $g(X)$ un p^r-polynôme de $\mathbb{F}_{p^s}[X]$, de la forme $g(X) = X^{p^{2r}} - aX^{p^r} - bX$ avec $ab \neq 0$. (r et s désignent des entiers arbitraires.)

On sait que le polynôme $f(g(X))$ est hyponormal sur $\mathbb{F}_{p^s}$. On donne explicitement dans ce qui suit le plus petit des degrés des polynômes irréductibles de $\mathbb{F}_{p^s}[X]$ factorisant le polynôme $f(g(X))$. Ce degré sera appelé ci-après "*le degré minimum de* $f(g(X))$ *sur* $\mathbb{F}_{p^s}$". *Ces hypothèses et cette terminologie sont supposées fixées dans tout ce qui suit.* Bon nombre de résultats sont établis lorsque la caractéristique p est différente de 2. Le cas $p = 2$ en conséquence fera l'objet d'une étude ultérieure.

Enfin on retrouve la même situation que celle qui avait été mise en évidence dans l'étude de la factorisation de $f(X^{p^r} - aX)$ [1], concernant le degré minimum. Ou bien ce degré est n, ou bien ce degré est de la forme $p^{k+1} \cdot n$, k étant un entier défini à l'aide de r, s et n.

N.B. Pour lire ce travail il faut d'abord se référer à [2]. Le lecteur peut en outre consulter [9] où les Auteurs étudient entre autres ce problème en imposant aux coefficients a et b l'appartenance au corps $\mathbb{F}_{p^{(s,n)}}$. On notera que nos résultats sont obtenus en toute généralité du moins *sans la restriction précédente.* Par ailleurs on a cherché une explicitation on ne peut plus poussée des paramètres.

0022-314X/80/040447-13$02.00/0

1. Résultat Fondamental

On dénote par α, β deux éléments de $\mathbb{F}_p$ tels que:

$$X^{p^{2r}} - aX^{p^r} - bX = (X^{p^r} - \alpha X)^{p^r} - \beta(X^{p^r} - \alpha X),$$

c'est-à-dire tels que $\alpha^{p^r} + \beta = a$ et $\alpha\beta = -b$. On a alors la proposition.

1.1. Proposition. *Soient*

$$u(X) = \sum_{t=0}^{[2r,sn]/r-2} \left(\sum_{h=t+1}^{[2r,sn]/r-1} \alpha^{(p^{[2r,sn]} - p^{(h+1)r})/(p^r-1)} \beta^{(p^{hr} - p^{(t+1)r})/(p^r-1)} \right) X^{p^{tr}},$$

$$v = -\alpha \sum_{h=1}^{[2r,sn]/r-1} \alpha^{(p^{[2r,sn]} - p^{(h+1)r})/(p^r-1)} \beta^{(p^{hr}-1)/(p^r-1)},$$

$$w = \sum_{h=0}^{[2r,sn]/r-1} \alpha^{(p^{[2r,sn]} - p^{(h+1)r})/(p^r-1)} \beta^{(p^{hr}-1)/(p^r-1)},$$

respectivement des éléments de $\mathbb{F}_{p^s}[X]$ et de $\mathbb{F}_{p^s}$. Soit $\theta \in \mathbb{F}_{p^{sn}}$ une racine du polynôme irréductible $f(X)$ de $\mathbb{F}_{p^s}[X]$ alors on a:

Cas 1: *Si* $(v-1)^{p^r+1} + a(v-1)w^{p^r} - bw^{p^r+1} \neq 0$ *alors le degré minimum de* $f(g(X))$, *sur* $\mathbb{F}_{p^s}$ *est n. De plus* $g(X) - \theta$ *possède une racine unique* x_0 *dans* $\mathbb{F}_{p^{sn}}$ *égale à*

$$x_0 = \frac{wu(\theta)^{p^r} - ((v-1)^{p^r} + aw^{p^r})\,u(\theta) + w^{p^r+1}\theta}{(v-1)^{p^r+1} + a(v-1)\,w^{p^r} - bw^{p^r+1}}.$$

Cas 2: *Si* $p \neq 2$, *si* $(v-1)^{p^r+1} + a(v-1)\,w^{p^r} - bw^{p^r+1} = 0$, *et si* $f(X) \nmid w(u(X))^{p^r} - ((v-1)^{p^r} + aw^{p^r})\,u(X) + w^{p^r+1}X$, *alors le degré minimum de* $f(g(X))$ *sur* $\mathbb{F}_{p^s}$ *est* $p^{k+1} \cdot n$ *où* p^k *est la plus grande puissance de p divisant* $2r/(2r, sn)$.

Cas 3: *Si* $p \neq 2$, *si* $(v-1)^{p^r+1} + a(v-1)\,w^{p^r} - bw^{p^r+1} = 0$, *si* $f(X) \mid w(u(X))^{p^r} - ((v-1)^{p^r} + aw^{p^r})\,u(X) + w^{p^r+1}X$, *si* $w \neq 0$, *alors le degré minimum de* $f(g(X))$ *sur* $\mathbb{F}_{p^s}$ *est n.*

Cas 4: *Si* $v = 1$, *si* $w = 0$ *et si* $f(X) \nmid u(X)$ *alors le degré minimum de* $f(g(X))$ *sur* $\mathbb{F}_{p^s}$ *est* $p^{k+1}n$, *où k est le plus grand exposant tel que* p^k *divise* $2r/(2r, sn)$.

Enfin,

Cas 5: *Si* $p \neq 2$, $v = 1$, $w = 0$ *et si* $f(X) \mid u(X)$ *alors le degré minimum de* $f(g(X))$ *sur* $\mathbb{F}_{p^s}$ *est n.*

Preuve. Elle va nécessiter de nombreux lemmes.

2. Lemmes

2.1. Lemme. *Soit $\theta \in \mathbb{F}_{p^{sn}}$ une racine du polynôme irréductible $f(X)$ de $\mathbb{F}_{p^s}[X]$. Soit l un entier non nul; on a dans $\mathbb{F}_{p^{sn}}[X]$ l'identité*

$$\begin{aligned} X^{p^{(l+1)r}} = &\sum_{t=0}^{l-1} \left(\sum_{h=t+1}^{l} \alpha^{(p^{(l+1)r}-p^{(h+1)r})/(p^r-1)} \beta^{(p^{hr}-p^{(t+1)r})/(p^r-1)} \right) \theta^{p^{rt}} \\ &- \alpha \left(\sum_{h=1}^{l} \alpha^{(p^{(l+1)r}-p^{(h+1)r})/(p^r-1)} \beta^{(p^{hr}-1)/(p^r-1)} \right) X \\ &+ \left(\sum_{h=0}^{l} \alpha^{(p^{(l+1)r}-p^{(h+1)r})/(p^r-1)} \beta^{(p^{hr}-1)/(p^r-1)} \right) X^{p^r} \\ &+ \sum_{t=0}^{l-1} \left(\sum_{h=t+1}^{l} \alpha^{(p^{(l+1)r}-p^{(h+1)r})/(p^r-1)} \beta^{(p^{hr}-p^{(t+1)r})/(p^r-1)} \right) \\ &\times (X^{p^{2r}} - aX^{p^r} - bX - \theta)^{p^{rt}}. \end{aligned}$$

La formule se démontre aisément en raisonnant par récurrence sur l'entier l. On écrira *provisoirement* pour alléger les notations:

$$X^{p^{(l+1)r}} = u_l(\theta) + v_l X + w_l X^{p^r} + u_l(X^{p^{2r}} - aX^{p^r} - bX - \theta)$$

avec $u_l(X) = \sum_{t=0}^{l-1} \left(\sum_{h=t+1}^{l} \alpha^{(p^{(l+1)r}-p^{(h+1)r})/(p^r-1)} \beta^{(p^{hr}-p^{(t+1)r})/(p^r-1)} \right) X^{p^{rt}}$. Ceci étant on a l'identité dans $\mathbb{F}_{p^s}[X]$:

$$X^{p^{(l+1)r}} = v_l X + w_l X^{p^r} + u_l(X^{p^{2r}} - aX^{p^r} - bX),$$

ce qui montre que $v_l, w_l \in \mathbb{F}_{p^s}$ et que $u_l(X) \in \mathbb{F}_{p^s}[X]$ pour tout $l \geqslant 1$. On a également: $v_l = -\alpha w_l + \alpha^{(p^{(l+1)r}-1)/(p^r-1)}$. On a donc: $v = v_{[2r,sn]/r-1}$, $w = w_{[2r,sn]/r-1}$ et $u(X) = u_{[2r,sn]/r-1}(X)$.

2.2. Lemme. *Le polynôme $u(X)$ de $\mathbb{F}_{p^s}[X]$ et les éléments v, w de $\mathbb{F}_{p^s}$ possèdent les propriétés suivantes*:

$$u(g(X)) + (v-1)X + wX^{p^r} = X^{p^{[2r,sn]}} - X, \tag{1}$$

$$g(u(X)) + (v-1)X + w^{p^{2r}}X^{p^r} = X^{p^{[2r,sn]}} - X, \tag{2}$$

$$w^{p^{2r}}a^{p^r} - aw^{p^r} + (v-1)^{p^{2r}} = v - 1, \tag{3}$$

$$w^{p^{2r}}b^{p^r} - bw + a(v-1) = a(v-1)^{p^r}. \tag{4}$$

Preuve. La propriété (1) n'est pas autre chose que l'identité du Lemme 2.1, avec $l = [2r, sn]/r - 1$, en utilisant la propriété que le polynôme $u(X)$ est un p^r-polynôme de $\mathbb{F}_{p^s}[X]$.

Pour démontrer (2)–(4), on procède de la manière suivante, on utilise l'identité de $\mathbb{F}_{p^s}[X, Y]$:

$$Y^{p^{[2r,sn]}} - Y = u(X) + (v-1)Y + wY^{p^r} + u(Y^{p^{2r}} - aY^{p^r} - bY - X),$$

on en déduit modulo $Y^{p^{2r}} - aY^{p^r} - bY - X$ les congruences:

$$(g(Y) - X)^{p^{[2r,sn]}} - (g(Y) - X) \equiv 0;$$

d'où

$$g(u(X) + (v-1)Y + wY^{p^r}) - X^{p^{[2r,sn]}} + X \equiv 0. \tag{5}$$

Or

$$Y^{p^{2r}} \equiv aY^{p^r} + bY + X,$$

et

$$Y^{p^{3r}} \equiv (a^{p^{r+1}} + b^{p^r})\, Y^{p^r} + a^{p^r} bY + a^{p^r} X + X^{p^r}.$$

Finalement on déduit de (5) que:

$$g(u(X)) + (w^{p^{2r}} a^{p^r} + (v-1)^{p^{2r}} - aw^{p^r})X + w^{p^{2r}} X^{p^r} = X^{p^{[2r,sn]}} - X, \tag{1'}$$

$$b(w^{p^{2r}} a^{p^r} + (v-1)^{p^{2r}} - aw^{p^r} - (v-1)) = 0, \tag{2'}$$

$$a(v-1)^{p^{2r}} + w^{p^{2r}}(a^{p^{r+1}} + b^{p^r}) - a(v-1)^{p^r} - a^2 w^{p^r} - bw = 0. \tag{3'}$$

Par conséquent, puisque $b \neq 0$, (1') et (2') fournissent

$$g(u(X)) + (v-1)X + w^{p^{2r}} X^{p^r} = X^{p^{[2r,sn]}} - X, \tag{2}$$

$$w^{p^{2r}} a^{p^r} - aw^{p^r} + (v-1)^{p^{2r}} = v - 1, \tag{3}$$

$$w^{p^{2r}} b^{p^r} - bw + a(v-1) = a(v-1)^{p^r}. \tag{4}$$

2.3. LEMME. *Soit $A - BX$ le reste de $g(X) - \theta$ dans la division euclidienne par $u(\theta) + (v-1)X + wX^{p^r}$ (ce dernier polynôme étant supposé non constant). Alors on a:*

$$(v-1)(w^{p^{2r}-1} B^{p^r} - B) = 0,$$

$$w^{p^{2r}} A^{p^r} + (v-1)A + w^{p^{2r}-1} u(\theta)\, B^{p^r} = 0;$$

Preuve. Par définition de A et B il est clair que $A, B \in \mathbb{F}_{p^{sn}}$. Procédons modulo $(u(\theta) + (v-1)X + wX^{p^r})$. On a les congruences

$$g(u(\theta) + (v-1)X + wX^{p^r}) \equiv 0,$$

donc

$$g(u(\theta)) + ((v-1)^{p^{2r}} - aw^{p^r})\, X^{p^{2r}} - (a(v-1)^{p^r} + bw)\, X^{p^r} - b(v-1)X + w^{p^{2r}} X^{p^{3r}} \equiv 0.$$

Mais avec les formules (3) et (4) du Lemme 2.2 on a:

$$g(u(\theta)) + (v - 1 - w^{p^{2r}} a^{p^r}) X^{p^{2r}} - (a(v-1) + w^{p^{2r}} b^{p^r}) X^{p^r} - b(v-1)X + w^{p^{2r}} X^{p^{3r}} \equiv 0,$$

soit à l'aide de la formule (2) du Lemme 2.2.

$$-w^{p^{2r}}\theta^{p^r} + (v-1)(A - BX) - w^{p^{2r}} a^{p^r} X^{p^{2r}} - w^{p^{2r}} b^{p^r} X^{p^r} + w^{p^{2r}} X^{p^{3r}} \equiv 0,$$

soit

$$-w^{p^{2r}}\theta^{p^r} + (v-1)(A - BX) + w^{p^{2r}}(X^{p^{2r}} - aX^{p^r} - bX)^{p^r} \equiv 0,$$

soit

$$-w^{p^{2r}}\theta^{p^r} + (v-1)(A - BX) + w^{p^{2r}}(\theta + A - BX)^{p^r} \equiv 0,$$

ou encore

$$(v-1)(A - BX) + w^{p^{2r}}(A - BX)^{p^r} \equiv 0.$$

Mais $wX^{p^r} \equiv -(v-1)X - u(\theta)$. Par conséquent

$$(v-1)(A - BX) + w^{p^{2r}} A^{p^r} + w^{p^{2r}-1} B^{p^r}((v-1)X + u(\theta)) = 0,$$

soit:

$$w^{p^{2r}} A^{p^r} + (v-1)A + w^{p^{2r}-1} u(\theta)\, B^{p^r} = 0$$

et

$$(v-1)(w^{p^{2r}-1} B^{p^r} - B) = 0.$$

Etablissons maintenant les expressions de A et de B. Si $w \neq 0$, on a

$$X^{p^r} \equiv -\frac{(v-1)}{w} X - \frac{u(\theta)}{w} \bmod(wX^{p^r} + (v-1)X + u(\theta)).$$

D'où

$$X^{p^{2r}} \equiv \left(\frac{v-1}{w}\right)^{p^r+1} X + \left(\frac{v-1}{w}\right)^{p^r} \cdot \frac{u(\theta)}{w} - \left(\frac{u(\theta)}{w}\right)^{p^r} \cdot \bmod(wX^{p^r} + (v-1)X + u(\theta)).$$

Et donc

$$\left(\frac{v-1}{w}\right)^{p^r+1} + a\left(\frac{v-1}{w}\right) - b = -B,$$

et

$$\left(\frac{v-1}{w}\right)^{p^r}\frac{u(\theta)}{w}-\left(\frac{u(\theta)}{w}\right)^{p^r}+a\frac{u(\theta)}{w}-\theta=A.$$

Si $w=0$, et $v\neq 1$, alors $A=-g(u(\theta)/(v-1))-\theta$, et $B=0$.

2.3.1. LEMME. *Avec les notations du Lemme* 2.3 *on a: si* $B\neq 0$, *alors* $g(X)-\theta$ *a une racine dans* $\mathbb{F}_{p^{sn}}$ *égale à* A/B.

Supposons donc $B\neq 0$. Si $w\neq 0$, le Lemme 2.3 fournit

$$w\left(\frac{A}{B}\right)^{p^r}+(v-1)\frac{A}{B^{p^r}w^{p^{2r}-1}}+u(\theta)=0,$$

si, de plus $v\neq 1$ alors $w^{p^{2r}-1}B^{p^r}=B$, et donc A/B est une racine $\in\mathbb{F}_{p^{sn}}$ de $wX^{p^r}+(v-1)X+u(\theta)$. Comme $g(X)-\theta\equiv A-BX \mod(wX^{p^r}+(v-1)X+u(\theta))$, il en résulte que $A-BX\mid g(X)-\theta$. Si $w\neq 0$ et $v=1$, le Lemme 2.2 fournit:

$$\begin{aligned}g(u(\theta))&=-w^{p^{2r}}\theta^{p^r},\\ w^{p^{2r}}a^{p^r}&=aw^{p^r},\\ w^{p^{2r}}b^{p^r}&=bw.\end{aligned}$$

Si on pose $u(\theta)=\xi^{p^r}$ et $w=w'^{p^r}$, ξ, $w'\in\mathbb{F}_{p^{sn}}$ alors:

$$(u(\theta))^{p^{2r}}-w^{p^{2r}-p^r}a^{p^r}u(\theta)^{p^r}-w^{p^{2r}-1}b^{p^r}u(\theta)=-w^{p^{2r}}\theta^{p^r},$$

soit

$$\xi^{p^{2r}}-aw'^{p^{2r}-p^r}\xi^{p^r}-w'^{p^{2r}-1}b\xi=-w^{p^r}\theta=-w'^{p^{2r}}\theta.$$

On en déduit que:

$$\left(\frac{\xi}{-w'}\right)^{p^{2r}}-a\left(\frac{\xi}{-w'}\right)^{p^r}-b\left(\frac{\xi}{-w'}\right)-\theta=0,$$

et donc $g(X)-\theta$ a une racine dans $\mathbb{F}_{p^{sn}}$. On vérifiera ci-dessous (cf. cas 1) que $-\xi/w'=A/B$.

Remarque. Si $w=0$ et $v\neq 1$. Le Lemme 2.2, formule 2, fournit:

$$-g\left(\frac{u(\theta)}{v-1}\right)-\theta=0;\qquad \text{ainsi}\quad A=0 \text{ et } B=0,$$

car $v-1\in\mathbb{F}_{p^r}$. On peut également utiliser le Lemme 2.3.

Nous sommes maintenant en mesure de démontrer le cas (1) de la Proposition 1.1.

Preuve du Cas 1 *de la Proposition* 1.1

Si $w \neq 0$ et $(v-1)^{p^r+1} + a(v-1)\, w^{p^r} - bw^{p^r+1} \neq 0$ et $v \neq 1$,

$$\frac{A}{B} = \frac{wu(\theta)^{p^r} - ((v-1)^{p^r} + aw^{p^r})\, u(\theta) + w^{p^r+1}\theta}{(v-1)^{p^r+1} + a(v-1)\, w^{p^r} - bw^{p^r+1}} = x_0.$$

L'unicité est immédiate car d'une part:

$$g(X) - \theta \equiv A - BX \bmod(u(\theta) + (v-1)X + wX^{p^r})$$

et d'autre part si $g(X) - \theta$ a une racine dans $\mathbb{F}_{p^{sn}}$ alors elle est racine de $u(\theta) + (v-1)X + wX^{p^r}$ donc de $A - BX$.

Si $w \neq 0$ et si $v = 1$, alors $(v-1)^{p^r+1} + a(v-1)\, w^{p^r} - bw^{p^r+1} \neq 0$; et on a

$$\frac{wu(\theta)^{p^r} - aw^{p^r}u(\theta) + w^{p^r+1}\theta}{-bw^{p^r+1}} = \frac{A}{B}.$$

Mais

$$\left(\frac{wu(\theta)^{p^r} - aw^{p^r}u(\theta) + w^{p^r+1}\theta}{-bw^{p^r+1}}\right)^{p^r} = -\frac{u(\theta)}{w}.$$

(En effet cette égalité n'est autre que la formule (2) du Lemme 2.2, avec $v = 1$, par suite $(A/B) = -\xi/w'$ et $x_0 = -\xi/w'$ (Lemme 2.3).)

Enfin si $w = 0$ et $v \neq 1$,

$$\frac{wu(\theta)^{p^r} - ((v-1)^{p^r} + aw^{p^r})\, u(\theta) + w^{p^r+1}\theta}{(v-1)^{p^r+1} + a(v-1)\, w^{p^r} - bw^{p^r+1}} = -\frac{u(\theta)}{v-1};$$

ce qui fournit une racine dans $\mathbb{F}_{p^{sn}}$ de $g(X) - \theta$ (Lemme 2.3.1). On observera, que dans ce cas il y a encore unicité car

$$X^{p^{[2r,sn]}} - X = u(\theta) + (v-1)X + u(g(X) - \theta).$$

Preuve du Cas 2 *de la Proposition* 1.1

Si $w \neq 0$ alors $(v-1)^{p^r+1} + a(v-1)\, w^{p^r} - bw^{p^r+1} = 0$ entraîne que $B = 0$. La deuxième condition $f(X) \nmid w(u(X))^{p^r} - ((v-1)^{p^r} + aw^{p^r})\, u(X) + w^{p^r+1}X$ signifie que $A \neq 0$. On a donc $g(X) - \theta \equiv A \bmod(u(\theta) + (v-1)X + wX^{p^r})$. Ainsi $g(X) - \theta$ est premier à $u(\theta) + (v-1)X + wX^{p^r}$.

Comme (Lemme 2.2; (1)) $u(g(X) - \theta) + u(\theta) + (v-1)X + wX^{p^r} = X^{p^{[2r,sn]}} - X$, alors $g(X) - \theta$ est premier à $X^{p^{[2r,sn]}} - X$. Mais on sait par [3] que si $p \neq 2$, $g(X) - \theta \mid X^{q^{\rho(q^6-1)}} - X$, avec $q = p^{[2r,sn]}$. Mais $g(X) - \theta$ est

hyponormal sur $\mathbb{F}_{p^{sn}}$. Donc son degré minimum sur $\mathbb{F}_{p^{sn}}$ est de la forme p^{α_0} avec

$$p^{\alpha_0} \nmid \frac{[2r, sn]}{sn} \qquad \text{et} \qquad p^{\alpha_0} \mid \frac{[2r, sn]}{sn}.$$

Donc si on considère le plus grand entier k, tel que $2r/(2r, sn) = p^k \times \omega$, $(p, \omega) = 1$, alors $p^k < p^{\alpha_0} \leqslant p^{k+1}$ d'où $\alpha_0 = k + 1$. Le degré minimum de $f(g(X))$ sur $\mathbb{F}_{p^s}$ est donc $p^{k+1}n$.

Si $w = 0$ et $(v-1)^{p^r+1} + a(v-1)w^{p^r} - bw^{p^r+1} = 0$, alors $v = 1$; la 2ème condition rejette ce cas car $f(X)$ divise 0.

Remarque. Si $w \neq 0$ alors $X^{p^r} - ((1-v)/w)X \mid g(X)$, et de plus $g(X)$ a une racine dans $\mathbb{F}^*_{p^{sn}}$.

Preuve du Cas 3 *de la Proposition* 1.1

Les conditions énoncées dans le cas 3, Proposition 1.1, montrent que:

$$u(\theta) + (v-1)X + wX^{p^r} \mid g(X) - \theta.$$

Par conséquent (en vertu de (1), Lemme 2.2) $u(\theta) + (v-1)X + wX^{p^r}$ divise $X^{p^{[2r,sn]}} - X$. Par ailleurs si $u(\theta) + (v-1)X + wX^{p^r}$ n'a pas de racine dans $\mathbb{F}_{p^{sn}}$ son degré minimum sur $\mathbb{F}_{p^{sn}}$, [1], est $p^{k'+1}$ où k' est tel que $r/(r, sn) = p^{k'} \cdot \omega'$ avec $(\omega', p) = 1$. (On aurait donc $p^{k'+1} \mid 2r/(2r, sn)$. Mais

$$\frac{2r}{(2r, sn)} = \frac{2}{(2, sn/(r, sn))} \cdot \frac{r}{(r, sn)} = \frac{2}{(2, sn/(r, sn))} p^{k'} \cdot \omega'.)$$

Comme on suppose $p \neq 2$ on a une contradiction. Donc $u(\theta) + (v-1)X + wX^{p^r}$ a une racine dans $\mathbb{F}_{p^{sn}}$, et a fortiori $g(X) - \theta$ aussi. On remarquera que dans ce cas

$$g(X) - \theta = \psi(u(\theta) + (v-1)X + wX^{p^r})$$

où ψ est un p^r-polynôme de $\mathbb{F}_{p^s}[X]$ que l'on peut expliciter. On a donc montré que le degré minimum sur $\mathbb{F}_{p^s}$ de $f(g(X))$ dans ce cas est n.

Remarque. On a encore $X^{p^r} - ((1-v)/w)X \mid g(X)$.

Preuve du Cas 4 *de la Proposition* 1.1

Avec les conditions énoncées on a la relation:

$$X^{p^{[2r,sn]}} - X = u(\theta) + u(g(X) - \theta).$$

Donc $g(X) - \theta$ est premier à $X^{p^{[2r,sn]}} - X$. Comme $g(X) - \theta \mid X^{q^p} - X$, on peut

reproduire le raisonnement (preuve du cas 2, Proposition 1.1), d'où le degré minimum de $f(g(X))$ sur $\mathbb{F}_{p^s}$ est donc $p^{k+1}n$.

Preuve du Cas 5 de la Proposition 1.1

Si $v=1$, $w=0$, $u(\theta)=0$, le Lemme 2.2 fournit les relations de commutation suivantes:

$$u(g(X)) = g(u(X)) = u(g(X)-\theta) = X^{p^{[2r,sn]}} - X.$$

Mais on peut écrire:

$$u(X) = u_1(\theta) + v_1 X + w_1 X^{p^r} + u_1(g(X)-\theta).$$

Soit

$$u(Y) = u_1(X) + v_1 Y + w_1 Y^{p^r} + u_1(g(Y)-X),$$

d'où

$$\begin{aligned} u(g(Y)-X) &= g(u(Y)) - u(X) \\ &\equiv g(u_1(X) + v_1 Y + w_1 Y^{p^r}) - u(X) \bmod (g(Y)-X), \end{aligned}$$

d'où par un calcul analogue à celui fait au début de ce travail:

$$u(X) = (u_1(X))^{p^{2r}} - a(u_1(X))^{p^r} - bu_1(X) + v_1 X + w_1^{p^{2r}} X^{p^r}.$$

On est alors amené à considérer différents sous-cas.

(1) Si $w_1 = 0$ et $v_1 \neq 0$ alors $g(X)-\theta$ a une racine dans $\mathbb{F}_{p^{sn}}$ égale à $-u_1(\theta)/v_1$.

(2) Si $w_1 = 0$, $v_1 = 0$ et $u_1(\theta) \neq 0$ alors $g(X)$ a une racine non nulle dans $\mathbb{F}_{p^{sn}}$ égale à $u_1(\theta)$.

On a donc

$$g(X) - \theta = (X^{p^r} - u_1(\theta)^{p^r-1} X)^{p^r} + b(u_1(\theta))^{1-p^r}(X^{p^r} - u_1(\theta)^{p^r-1} X) - \theta.$$

Considérons le polynôme $X^{p^r} + bu_1(\theta)^{1-p^r} X - \theta$ de $\mathbb{F}_{p^{sn}}[X]$. Si ce polynôme a une racine dans $\mathbb{F}_{p^{sn}}$, soit λ_0, alors $X^{p^r} - u_1(\theta)^{p^r-1} X - \lambda_0$ est dans $\mathbb{F}_{p^{sn}}[X]$ et divise $X^{p^{[2r,sn]}} - X$, puisque $g(X)-\theta$ divise $X^{p^{[2r,sn]}} - X$. On a vu alors, puisque $p \neq 2$, que cela entraînait l'existence d'un élément $x_0 \in \mathbb{F}_{p^{sn}}$ tel que $x_0^{p^r} - u_1(\theta)^{p^r-1} x_0 = \lambda_0$. Ainsi $g(x_0) = \theta$. On a ainsi montré que dans ce cas $g(X)-\theta$ a une racine dans $\mathbb{F}_{p^{sn}}$.

Si $X^{p^r} + bu_1(\theta)^{1-p^r} X - \theta$ n'a pas de racine dans $\mathbb{F}_{p^{sn}}$, alors on sait par [1] que nécessairement, il se décompose en irréductibles de $\mathbb{F}_{p^{sn}}[X]$ de degrés multiples de p^{k+1}, où k est la valuation de $r/(r, sn)$ ou $2r/(2r, sn)$ en p, (on a

$p \neq 2$). Soit donc un tel irréductible, désignons le par $f_1(X)$. Alors $f_1(X^{p^r} - u_1(\theta)^{p^r-1}X)$ se décompose lui aussi en irréductibles de $\mathbb{F}_{p^{sn}}[X]$ de degrés multiples de p^{k+1}. Mais $g(X) - \theta$, divise $X^{p^{[2r,sn]}} - X$ et p^{k+1} ne divise pas $2r/(2r, sn) = p^k \cdot \omega$; $((\omega, p) = 1)$, a fortiori cela est vrai pour les degrés des irréductibles de $\mathbb{F}_{p^{sn}}[X]$ factorisant $f_1(X^{p^r} - u_1(\theta)^{p^r-1}X)$. On obtient donc une contradiction.

(3) Si $w_1 = 0$, $v_1 = 0$ et $u_1(\theta) = 0$ alors $u(X) = u_1(g(X) - \theta)$. Il faut recommencer l'étude précédente à partir de $u_1(X)$. On reviendra plus loin sur ce cas.

(4) Si $w_1 \neq 0$, alors $g(X) - \theta \equiv A_1 - B_1X \bmod(u_1(\theta) + v_1X + w_1X^{p^r})$ et on peut reproduire les considérations développées dans le Lemme 2.3.1. De façon précise si $B_1 \neq 0$, alors $A_1 - B_1X \mid g(X) - \theta$ d'où $g(X) - \theta$ a une racine dans $\mathbb{F}_{p^{sn}}$. Si $B_1 = 0$ et $A_1 \neq 0$. On a $(-v_1/w_1)^{p^r+1} - a(-v_1/w_1) - b = B_1 = 0$.

On ne peut avoir $v_1 = 0$, donc $-v_1/w_1 = (w_1^{p^r+1}A_1)^{p^r-1}$ (Lemme 2.3). Ainsi $g(X)$ a une racine non nulle dans $\mathbb{F}_{p^{sn}}$, et comme dans (2) ci-dessus cela conduit à l'existence d'une racine, dans $\mathbb{F}_{p^{sn}}$ pour $g(X) - \theta$.

Si $A_1 = B_1 = 0$, alors $u_1(\theta) + v_1X + w_1X^{p^r}$ divise $g(X) - \theta$ donc divise $X^{p^{[2r,sn]}} - X$, et donc puisque $p \neq 2$, $g(X) - \theta$ a une racine dans $\mathbb{F}_{p^{sn}}$.

Il reste à régler le sous-cas 3.

Supposons que ce cas se présente constamment, c'est-à-dire que:

$$\begin{aligned} X^{p^{[2r,sn]}} - X = u(g(X)) = g(u(X)), &\qquad u(\theta) = 0, \\ u(X) = u_1(g(X)) = g(u_1(X)), &\qquad u_1(\theta) = 0, \\ \vdots \qquad\qquad \vdots &\qquad \vdots \\ u_{t-1}(X) = u_t(g(X)) = g(u_t(X)), &\qquad u_t(\theta) = 0. \end{aligned}$$

Les polynômes $u_t(X)$ ainsi définis sont des p^r-polynômes moniques de $\mathbb{F}_{p^s}[X]$. $u_t(X)$ a pour degré $p^{[2r,sn]-2(t+1)r}$. On aurait donc pour t_0 tel que $2(t_0 + 1)r = [2r, sn]$

$$X^{p^{[2r,sn]}} - X = g \circ g \circ \cdots \circ g(X),$$

avec $u_{t_0}(X) = X$ et $u_{t_0}(\theta) = 0$. Donc $f(X) = X$ et bien évidemment alors $f(X^{p^{2r}} - aX^{p^r} - bX) = X^{p^{2r}} - aX^{p^r} - bX$ a une racine dans $\mathbb{F}_{p^{sn}} = \mathbb{F}_{p^s}$. Si l'éventualité ci-dessus ne se produit pas, alors on est ramené à toute l'étude précédente avec un polynôme $u_t(X)$ pour un indice t convenable.

3. Exemples

Nous allons illustrer par des exemples numériques les différents cas de la Proposition 1.1.

3.1. *1er Cas.* Prenons $s = 2$, $r = 1$, $n = 1$, $p = 3$. Soit ξ un élément de $\mathbb{F}_{3^2}$

tel que $\xi^2 = 2$. Enfin soit $f(X) = X + 2\xi$ dans $\mathbb{F}_9[X]$ et $g(X) = X^{3^2} - \xi X^3 - \xi X$. Alors le polynôme $X^{3^2} - \xi X^3 - \xi X + 2\xi = f(g(X))$ est tel que:

$$X^{3^{[2r,sn]}} - X \equiv \xi + (\xi + 2)X + \xi X^3 \bmod(g(X) + 2\xi), \qquad \text{avec} \quad [2r, sn] = 2.$$

Ainsi $u(\theta) = \xi$, $v - 1 = \xi + 2$, $w = \xi$. Par suite $(v-1)^{p^r+1} + a(v-1)w^{p^r} - bw^{p^r+1} = 1$ et

$$wu(\theta)^{p^r} - ((v-1)^{p^r} + aw^{p^r})\,u(\theta) + w^{p^r+1}\theta = \xi.$$

D'où $x_0 = \xi$. Donc $X^{3^2} - \xi X^3 - \xi X + 2\xi$ admet ξ pour racine dans $\mathbb{F}_9$, et cette racine est unique.

3.2. *2ème Cas.* Prenons $s = 2$, $r = 1$, $n = 1$, $p = 3$. On a $[2r, sn] = 2$. Soit $f(X) = X + 2$ et $g(X) = X^{3^2} + \xi X^3 + X$ avec $\xi^2 = 2$, $\xi \in \mathbb{F}_9$.

On a $X^{3^{[2r,sn]}} - X = X^{3^2} - X \equiv 1 + X + 2\xi X^3 \bmod(g(X) - \theta)$.

Ainsi $u(\theta) = 1$, $v - 1 = 1$, $w = 2\xi$, et $a = 2\xi$, $b = -1$. Par suite

$$(v-1)^{p^r+1} + a(v-1)w^{p^r} - bw^{p^r+1} = 0,$$
$$w(u(\theta))^{p^r} - ((v-1)^{p^r} + aw^{p^r})\,u(\theta) + w^{p^r+1}\theta = 2\xi + 2 \neq 0.$$

La Proposition 1.1 affirme donc que $X^{3^2} + \xi X^3 + X + 2$ a 3 pour degré minimum sur $\mathbb{F}_{3^2}$. Ce degré divise donc les degrés des autres irréductibles. On a d'ailleurs $X^9 - X = 1 + X + 2\xi X^3 + X^{3^2} + \xi X^3 + X + 2$ et

$$X^{9^3} - X \equiv 0 \bmod(g(X) - \theta).$$

Par conséquent $X^{3^2} + \xi X^3 + X + 2$ est le produit de 3 irréductibles de $\mathbb{F}_9[X]$ de degrés 3.

3.3. *3ème Cas.* Prenons $p = 3$, $r = 1$, $s = 2$, $n = 1$. On a $[2r, sn] = 2$.

Soit ξ une racine de $X^2 - X - 1 \in \mathbb{F}_3[X]$. Ce polynôme est irréductible sur $\mathbb{F}_3$. Donc $\xi \in \mathbb{F}_9$ et $\xi \notin \mathbb{F}_3$. Soit θ une racine de $X^2 - 2 \in \mathbb{F}_3[X]$. 2 n'est pas un carré dans $\mathbb{F}_3$ donc $\theta \in \mathbb{F}_9$ et $\theta \notin \mathbb{F}_3$. Soient donc les polynômes $f(X) = X - \theta$ et $g(X) = X^{3^2} - \xi X^3 - \xi X$ de $\mathbb{F}_9[X]$. On a les relations

$$X^{3^2} - X \equiv \xi X^3 + (\xi - 1)X + \theta \bmod(g(X) - \theta)$$

et

$$g(X) - \theta = 2\xi(\xi X^3 + (\xi - 1)X + \theta)^3 + (2\xi + 2)(\xi X^3 + (\xi - 1)X + \theta).$$

On vérifie alors que, $u(\theta) = \theta$, $v = \xi$, $w = \xi \neq 0$ et

$$(v-1)^{p^r+1} + a(v-1)w^{p^r} - bw^{p^r+1} = 0,$$
$$wu(\theta)^{p^r} - ((v-1)^{p^r} + aw^{p^r})\,u(\theta) + w^{p^r+1}\theta = 0.$$

Alors le degré minimum de $f(g(X)) = X^{3^2} - \xi X^3 - \xi X - \theta$ sur $\mathbb{F}_9$ est 1. On a d'ailleurs $g(\theta) - \theta = 0$. En effet, θ est une racine de $\xi X^3 + (\xi - 1)X + \theta$. On voit que *tous* les degrés des irréductibles factorisant ce dernier polynôme, dans $\mathbb{F}_9[X]$, sont égaux à 1 car $(1 - \xi)/\xi$ est un carré dans $\mathbb{F}_9$.

3.4. *4ème Cas.* Prenons $p = 3$, $r = 1$, $s = 2$, $n = 2$. On a $[2r, sn] = 4$. Soient ξ et λ tels que $\xi^2 = 2$, $\lambda^2 + \lambda + 2 = 0$. $\xi, \lambda \in \mathbb{F}_{3^2}$ et $\xi, \lambda \notin \mathbb{F}_3$. Soit $g(X) = X^{3^2} - \xi X^3 - \lambda X$. Enfin soit $\theta \in \mathbb{F}_{9^2}$, $\theta \notin F_9$ tel que $\theta^2 = \lambda$. (λ n'est pas un carré dans $\mathbb{F}_9$). Soit $f(X) = X^2 - \lambda$. On a $u(X) = (\lambda + 1)X + \xi X^3 + X^{3^2}$, et $g(X) - \theta$ est tel que: $X^{3^4} - X = u(\theta) + u(g(X) - \theta)$. Ainsi $w = v - 1 = 0$. Enfin on a $u(\theta) = \lambda(\xi + 1)\theta \neq 0$. Donc $f(g(X)) = (X^{3^2} - \xi X - \lambda X)^2 - \lambda$ possède un facteur irréductible de degré 6 sur $\mathbb{F}_{3^2}$, et c'est le degré minimum. Comme $u(\theta) \in \mathbb{F}_{3^4}$ on en déduit que $g(X) - \theta \mid X^{(3^4)^3} - X$. Comme $u(\theta) \neq 0$, $g(X) - \theta$ ne peut avoir de racine dans $\mathbb{F}_{3^4}$, et donc $g(X) - \theta$ est le produit de 3 irréductibles de degrés 3 sur $\mathbb{F}_{3^4}$.

3.5. *5ème Cas.* Prenons $p = 3$, $s = 4$, $r = 3$. Soit a une racine du polynôme $X^4 - X^2 - 1$, qui est irréductible sur $\mathbb{F}_3$. Ainsi $a^8 = -1$ et $a^{16} = 1$ et $a \in \mathbb{F}_{3^4}$ et $a \notin \mathbb{F}_{3^2}$. Soit $b = a^4$, enfin on a donc $b^2 = -1$. a n'est pas un carré dans $\mathbb{F}_{3^4}$ car $a^{(9^2-1)/2} = a^{40} = (a^8)^5 = -1$.

Le polynôme $X^2 - a$ est donc irréductible sur $\mathbb{F}_{3^4}$. Soit θ l'une de ses racines dans $\mathbb{F}_{3^8}$. Enfin soit $g(X) = X^{3^6} - aX^{3^3} - bX$. On a donc $n = 2$ et $[2r, sn] = [6, 8] = 24$. On vérifie que $X^{3^{24}} - X = (g(g(X))^{3^{12}} + g(g(X))$. Ainsi $v = 1$, $w = 0$, et $u(X) = (g(X))^{3^{12}} + g(X)$. Comme $u(\theta) = 0$, la Proposition 1.1 assure l'existence d'une racine dans F_{3^8} pour $g(X) - \theta$. Le degré minimum de $(X^{3^6} - aX^{3^3} - bX)^2 - a$ sur $\mathbb{F}_{3^4}$ est donc 2. On a d'ailleurs $g(-\theta) - \theta = 0$, et donc $X^2 - a$ divise $(X^{3^6} - aX^{3^3} - bX)^2 - a$.

4. Remarques

Du développement de cet article, on peut dégager les remarques suivantes:

Si $g(X)$ possède une racine ξ non nulle telle que $\xi^{p^r - 1}$ appartienne à l'extension $\mathbb{F}_{p^{sn}}$ de $\mathbb{F}_{p^s}$, alors

$$X^{p^{2r}} - aX^{p^r} - bX = (X^{p^r} - \xi^{p^r - 1}X)^{p^r} + b\xi^{1-p^r}(X^{p^r} - \xi^{p^r-1}X)$$
$$= (X^{p^r} - \xi^{p^r-1}X)[(X^{p^r} - \xi^{p^r-1}X)^{p^r-1} + b\xi^{1-p^r}]$$

et on sait par [2] que $(X^{p^r} - \xi^{p^r-1}X)^{p^r-1} + b\xi^{1-p^r}$ est lui aussi hyponormal sur $\mathbb{F}_{p^{sn}}$. On peut donc pousser plus loin l'explicitation des degrés pour $g(X)$.

On a ainsi (dans la mesure où ξ est explicitement connue, c'est-à-dire si on connait l'entier $[\mathbb{F}_{p^{sn}}(\xi) : \mathbb{F}_{p^{sn}}]$), théoriquement tous les degrés des irréductibles de $\mathbb{F}_{p^{sn}}[X]$ factorisant $g(X) - \theta$.

Dans le cas 1 de la Proposition 1.1, la connaissance explicite de $x_0 \in \mathbb{F}_{p^{sn}}$

permet de mettre en évidence un p^r-polynôme $h(X)$ de $\mathbb{F}_{p^s}[X]$, tel que le polynôme transformé de $f(X)$ par $h(X)$ soit lui aussi irréductible de degré n dans $\mathbb{F}_{p^s}[X]$. On avait déjà dans [1] mis en évidence un p^r-polynôme possédant cette propriété.

Enfin dans le cas 5 de la Proposition 1.1, c'est-à-dire lorsque $g(X) - \theta$ divise $X^{p^{[2r,sn]}} - X$, il est aisé de voir que

$$\alpha^{(p^{[2r,sn]}-1)/(p^r-1)} = \beta^{(p^{[2r,sn]}-1)/(p^r-1)} = 1,$$

et donc que

$$(-b)^{(p^{[2r,sn]}-1)/(p^r-1)} = 1.$$

Le polynôme $u(X)$ de $\mathbb{F}_{p^{sn}}[X]$ a des coefficients qui sont des fonctions polynômes de α puisque $\beta = -b/\alpha$. On peut donc par division par $X^{p^r+1} - aX - b$, exprimer ces coefficients à l'aide de a et b: ce sont en effet les restes de ces divisions.

BIBLIOGRAPHIE

1. S. AGOU, Factorisation sur un corps fini $\mathbb{F}_{p^n}$ des polynômes composés $f(X^{p^r} - aX)$ lorsque $f(X)$ est un polynôme irréductible de $\mathbb{F}_{p^n}[X]$, *J. Number Theory* **9** (1977), 229–239.
2. S. AGOU, Sur une classe de polynômes hyponormaux sur un corps fini, A paraître dans *Acta Arith.* **39**, n° 2.
3. S. AGOU, Irréductibilité des polynômes $f(\sum_{i=0}^{m} a_i X^{p^{ri}})$ sur un corps fini $\mathbb{F}_{p^s}$, *Canad. Math. Bull.* **23**(2) (1980), 207–212.
4. L. CARLITZ ET A. F. LONG, The factorization of $Q(L(x_i),..., L(x_k))$ over a finite field where $Q(x_1,..., x_k)$ is of first degree and $L(x)$ is linear, *Acta Arith.* **32** (1977), 407–420.
5. R. CHURCH, Tables of irreducible polynomials for the first four prime moduli, *Ann. Math.* **36**, n° 1 (January 1935).
6. L. E. DICKSON, "Linear Groups with an Exposition of the Galois Field Theory," Dover, New York.
7. A. F. LONG, Classification of irreducible factorable polynomials over a finite field, *Acta Arith.* **12** (1967), 301–313.
8. A. F. LONG, A theorem on factorable irreducible polynomials in several variables over a finite Field with the substitution $x_i^{q^r} - x_i$ for x_i, *Math. Nachr.* **63** (1974), 123–130.
9. A. F. LONG AND T. P. VAUGHAN, Factorization of $Q(h(T)(x))$ over $GF(q)$ where $Q(x)$ is irreducible and $h(T)(x)$ is linear, I, II, *Linear Algebra Appl.* **13** (1976), 207–221; **11** (1975), 53–72.
10. O. ORE, Contributions to the theory of finite fields, *Trans. Amer. Math. Soc.* **36** (1934), 243–274.